PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-157223
(43)Date of publication of application : 31.05.2002

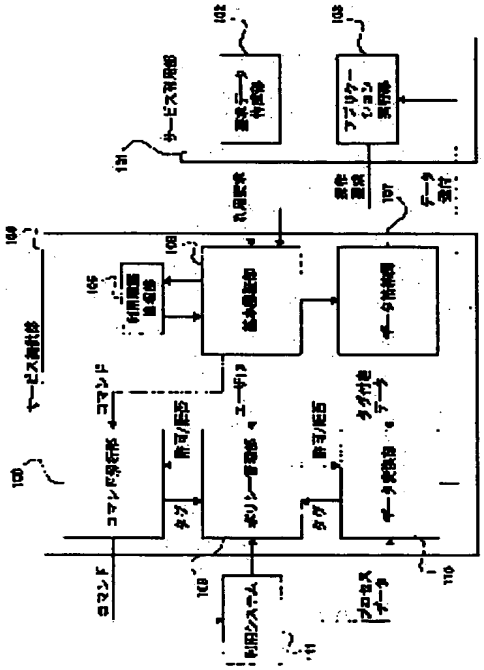
(51)Int.Cl. G06F 15/00
G06F 17/30
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 2000-355635
(22)Date of filing : 17.11.2000

(71)Applicant : HITACHI LTD
(72)Inventor : KATO HIROMITSU
FURUYA MASATOSHI
SEKOZAWA TERUJI
MIYAO TAKESHI

(54) SERVICE PROVIDING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To dynamically select information to be transmitted/received according to the authority of a user, and to prevent the same operation from being received plural times by erroneous operation.
SOLUTION: In a request data preparing part 102, service utilization request data are prepared and sent to a basic authentication part 106. In the basic authentication part 106, the user is authenticated, and in respect to a legal user, a service utilization request is accepted. Requested data are retrieved by a data storage part 107 and dispatched to a data converting part 110. The data converting part 110 inquires whether tagged data can be provided to the user or not to a policy managing part 109. Corresponding to the user ID of the user, the tag and the state of a utilization system 111, the policy managing part 109 judges permission/refusal and the data converting part 110 converts data so that data permitted by the policy managing part 109 can be disclosed and refused data can be hidden, and provides the data to an application executing part 103.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－157223
（P2002－157223A）
(43)公開日　平成14年５月31日(2002.5.31)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｂ	５Ｂ０７５
	17/30	１１０	17/30	１１０Ｆ	５Ｂ０８５
		１２０		１２０Ｂ	５Ｊ１０４
				１２０Ａ	
		２４０		２４０Ｃ	

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願2000－355635(P2000－355635)

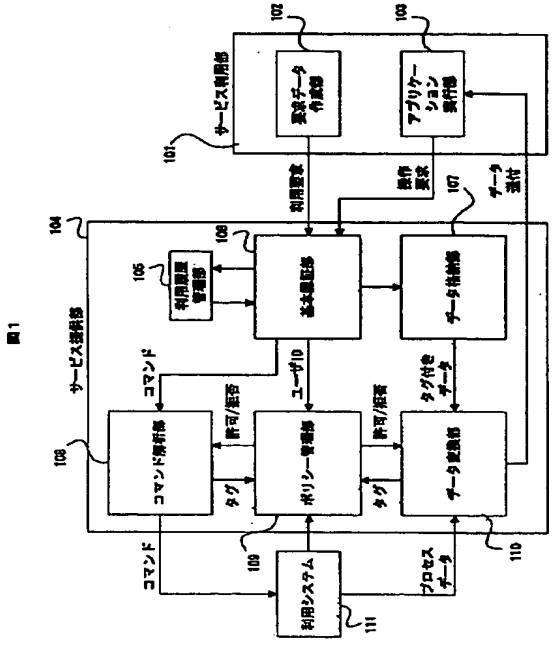
(22)出願日　平成12年11月17日(2000.11.17)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　加藤　博光
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　古谷　雅年
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　サービス提供システム

(57)【要約】
【課題】利用者の権限に沿って送受信する情報を動的に取捨選択し、かつ、誤操作による同じ操作の複数回受信を防止する。
【解決手段】要求データ作成部１０２においてサービス利用要求データを作成し、基本認証部１０６に送る。基本認証部１０６では利用者を認証し、正当な利用者に対してサービス利用要求を受け付ける。要求されたデータをデータ格納部１０７は検索し、データ変換部１１０に渡す。データ変換部１１０はタグ付けされたデータを利用者に提供して良いかポリシー管理部１０９に問い合わせる。ポリシー管理部１０９は、利用者のユーザＩＤとタグ、および利用システム１１１の状態によって許可・拒否の判断を下し、データ変換部１１０はポリシー管理部１０９によって許可されたデータを開示し、拒否されたデータは隠蔽するようにデータを変換し、アプリケーション実行部１０３にデータを提供する。



【特許請求の範囲】
【請求項１】利用者に対して所定のサービスを提供するための情報処理を実行するサービス提供システムであって、
前記サービスを提供するためのサービス情報を格納する手段と、
前記サービス内容を要求する要求情報、前記利用者の特徴を示すユーザ属性および前記利用者を認証する認証子を含む要求データを受付ける手段と、
前記ユーザ属性および前記認証子に基づいて、前記利用者を認証する手段と、
前記認証の結果に基づいて、前記サービス情報に含まれる情報に対する前記利用者のアクセス可否を決定する手段と、
前記要求情報に対応するサービス情報を、前記アクセス可能なサービス情報から検索する手段と、
検索された前記サービス情報を、決定された前記アクセス可否に適応するよう変換する手段と、
変換された前記サービス情報を提示する手段とを有することを特徴とするサービス提供システム。
【請求項２】請求項１に記載のサービス提供システムにおいて、
前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合には、２回目以降に入力された要求データの受信を抑止することを特徴とするサービス提供システム。
【請求項３】請求項２に記載のサービス提供システムにおいて、
前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合、前記利用者から複数入力することを確認することが入力された場合は、前記２回目以降に入力された要求データを受信することを特徴とするサービス提供システム。
【請求項４】請求項３に記載のサービス提供システムにおいて、
前記受付ける手段は、前記要求データの内容の同じものが複数入力された場合には、前記利用者に対して、複数入力であることを示す情報を提示することを特徴とするサービス提供システム。よって利用可能な前記データ属性を制限する機能を有することを特徴とする請求項１乃至２に記載のサービス提供システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はコンテンツの配信およびコンテンツの利用をサービスとして提供するサービス提供システムに関し、特に、権利のあるものに適切にサービスを提供することでプライバシーの保護、コンテンツの不正利用防止を行なうサービス提供システムに関する。
【０００２】
【従来の技術】インターネットに代表される情報通信技術の発展によって、ネットワークを介して音楽やゲームなどのコンテンツを配信したり、インターネットバンキングのように携帯電話や自宅のパソコンから残高照会や振込みを行なえるサービスが一般に普及してきている。ところが、サービス利用者が不特定多数となることで、サービス利用者の多様なニーズに対応するとともに、情報セキュリティ上の脅威への対策を十分に考慮していく必要がでてきた。
【０００３】多様なニーズへの対応として、例えば特開２０００－８２０３９号「表示制御情報生成方法およびコンピュータ」に示されるように、様々な能力を有するクライアント端末に対して、それぞれの能力に応じたユーザインターフェースを提供するために、端末属性情報を参照してＨＴＭＬ等の表示制御情報を動的に生成するものがある。
【０００４】また情報セキュリティを確保するための技術として、特開２０００－１９９６０号では「遠隔操作方法」を次のように記している。すなわち、操作端末から制御装置に制御信号を送信する際に、ユーザが制御信号を入力すると、次回操作権を発生し、制御装置側では制御信号と次回操作権と今回操作権を含む信号を共通鍵で暗号化し、操作端末に転送する。次回操作権は操作端末に記憶する。制御装置側では転送された暗号文を共通鍵で復号化し、制御信号と今回操作権と次回操作権とを取得し、今回操作権が制御装置側に登録してある操作権と一致するかを判定し、一致する場合は制御機器に制御信号を送る。次回操作権は制御装置側に登録される。
【０００５】
【発明が解決しようとする課題】かかる従来方法においては次のような問題がある。すなわち、特開２０００－８２０３９号に関しては、コンテンツを提供する際には、クライアント端末から送信される端末属性情報に基づいて提供するコンテンツを動的に生成するが、端末を利用して閲覧している利用者がそのコンテンツを閲覧する権限があるかどうかが加味されない。コンテンツが重要な機密情報を含んでいるもの、プライバシーの保護が必要なもの、会員のみに限定して提供するもの等の場合には、提供相手となるコンテンツ利用者の権限を考慮してコンテンツを生成・配信を行なう必要がある。
【０００６】また、特開２０００－１９９６０号に関しては、操作端末から誤って複数回同じ操作を行なった場合、制御装置は正当な制御信号が複数回送られてきたと認識して、同じ制御を繰り返し実行してしまう可能性がある。例えば、インターネットバンキングに本手法を適用すると、振込み操作信号を誤って複数回送信してしまった場合には、それを検知することなく、必要以上に多額の振込みをしてしまうという問題があった。
【０００７】本発明の目的は、利用者の権限に沿って提供する情報、受け取る情報を動的に取捨選択するサービ

ス提供システムを提供することにある。

【０００８】本発明の他の目的は、サービス利用時に誤って同じ制御信号を複数回送信してしまった場合にも、利用者の確認無しには複数回受け付けないサービス提供システムを提供することにある。

【０００９】

【課題を解決するための手段】本発明は、利用者に対して所定のサービスを提供するための情報処理を実行するサービス提供システムであって、前記サービスを提供するための複数のサービス情報を格納する手段と、前記サービス内容を要求する要求情報、前記利用者の特徴を示すユーザ属性および前記利用者を認証する認証子を含む要求データを受付ける手段と、前記ユーザ属性および前記認証子に基づいて、前記利用者を認証する手段と、前記認証の結果に基づいて、前記サービス情報に含まれる情報に対する前記利用者のアクセス可否を決定する手段と、前記要求情報に対応するサービス情報を、前記アクセス可能なサービス情報から検索する手段と、検索された前記サービス情報を、決定された前記アクセス可否に適応するよう変換する手段と、変換された前記サービス情報を提示する手段とを有する。なお、変換には、アクセス可能な情報を表示可能とし、アクセス不可能な情報の表示を抑止することを含む。

【００１０】また、本発明の別の形態では、同じ要求データの受信を抑止することを特徴とする。

【００１１】他、以下のサービス提供システムも本発明に含まれる。ユーザ属性と認証子を添付してリクエストを作成する要求データ作成部と、ユーザ属性と認証子からユーザ認証を行なう基本認証部と、アクセス可能なデータ属性を指定するポリシー管理部と、リクエストに基づいて要求されるデータを取り出すデータ格納部と、ポリシー管理部によって指定されたデータ属性に従ってデータを再構築してユーザに提供するデータ変換部を有するサービス提供システム。

【００１２】また、送達確認値と、データ属性によって特徴付けられた操作要求に、ユーザ属性と認証子を添付して送信するアプリケーション実行部と、ユーザ属性と認証子からユーザ認証を行なう基本認証部と、送達確認値が受信済みのものでないかチェックを行なう利用履歴管理部と、アクセス可能なデータ属性を指定するポリシー管理部と、操作要求を解析しポリシー管理部の判断に基づいて利用システムを操作するコマンド解析部を有するサービス提供システム。

【００１３】さらに、上記のサービス提供システムそれぞれにおいて、ポリシー管理部が、ユーザ属性によって利用可能なデータ属性を制限する機能と、利用システムの状態によって利用可能なデータ属性を制限する機能を有する。

【００１４】さらに、基本認証部が、送達確認値を更新する機能と、送達確認値を利用者のみが復号化できる形で暗号化する機能を有するサービス提供システムも本発明に含まれる。

【００１５】さらに、アプリケーション実行部が、基本認証部から返信された送達確認値を受信したことを確認する機能と、送達確認値を復号化して操作要求を次回送信のために保存する機能を有するサービス提供システムも本発明に含まれる。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。本発明の実施の一形態として、プラント監視制御システムに本発明を適用した場合のブロック図を図１に示す。図１にはサービス利用部１０１がサービス提供部１０４から情報を入手する手段と、サービス利用部１０１が利用システム１１１に対して操作を行なう手段とを記載している。

【００１７】サービス利用部１０１は、要求データ作成部１０２とアプリケーション実行部１０３からなる。要求データ作成部１０２は、利用者の要求をユーザＩＤ、パスワード等とともにサービス提供部１０６に送る。アプリケーション実行部１０３はサービス提供部１０６から渡されたデータを閲覧したり、利用システム１１１に対して操作を行なったりするものである。

【００１８】サービス提供部１０４は、利用履歴管理部１０５、基本認証部１０６、データ格納部１０７、ポリシー管理部１０９、データ変換部１１０、コマンド解析部１０８からなる。利用履歴管理部１０５は利用者の利用履歴を管理する。基本認証部１０６は利用者の認証を行なう。データ格納部１０７はデータを格納しておき要求に応じて必要なデータを検索する。ポリシー管理部１０９はデータ利用を許可するか拒否するかを判断する。データ変換部１１０は利用者が利用可能な形にデータを変換する。コマンド解析部１０８は、サービス利用部１０１から送られた利用システム１１１に対する操作コマンドを解析する。

【００１９】まず、サービス利用部１０１がサービス提供部１０４から情報を入手する処理フローを図２に従って説明する。サービス利用部１０１は、要求データ作成部１０２において認証情報を付与して提供して欲しいデータを指定し（ステップ２０１）、サービス提供部１０４に要求する（ステップ２０２）。基本認証部１０６でユーザ属性と認証子が正確に関連付いているかを確認し利用者の認証を行なう（ステップ２０３）。利用者が認証されると、基本認証部１０６はデータ格納部１０７に対してデータの検索要求を行なう（ステップ２０４）。データ格納部１０７は要求されたデータを検索する（ステップ２０５）。ここで、データ格納部１０７に格納されているデータは各データ要素を、データ属性としてタグによって特徴付けている。データ変換部１１０は、検索されたタグ付きデータのタグを読み取り（ステップ２０６）、各々のタグ付きデータを該当利用者に提供して

よいかどうかをポリシー管理部１０９に問い合わせる（ステップ２０７）。ポリシー管理部１０９は基本認証部１０６が認証したユーザＩＤとタグをもとにデータ提供の許可・拒否を判定する（ステップ２０８）。データ変換部１１０はポリシー管理部１０９の判定結果に基づき、許可するデータは開示し、拒否するデータは隠蔽する（ステップ２０９）。データ変換部１１０は、作成したデータを利用者に提供するために暗号通信を行なう（ステップ２１０）。暗号通信方法としてはＳＳＬ等の既存の手法を用いることができる。ここで、公開鍵暗号方式では、皆に公開できる公開鍵と、個人で秘密にしていなければならない秘密鍵をペアで用い、公開鍵で暗号化したデータは、対となる秘密鍵でないと元のデータに復号できないという性質がある。この性質を利用して、暗号通信に用いる暗号鍵を公開鍵で暗号化して渡すことによって、認証された利用者のみにデータを提供することができる。利用者の公開鍵は、信頼できる第三者機関が電子証明書を発行することによって鍵の持ち主を保証する。

【００２０】各処理ステップ毎の具体的なイメージを以下に示す。要求データ作成部１０２の具体例を図３に示す。図３では、ユーザ属性としてユーザＩＤ３０１、提供して欲しいデータとして利用希望サービスリスト３０３から要求データ３０４（ここでは「ポンプとバルブ」）を選択している。利用者の秘密鍵はパスワードによって暗号化されており、これを復号化するためにパスワード３０２を入力する項がある。復号化された秘密鍵は、ユーザＩＤ３０１と要求データ３０４に対してディジタル署名を行なうことに用いる。「ログイン」ボタン３０５を押すことにより、図４のように、ユーザＩＤ３０１と要求データ３０４のセット、これのディジタル署名４０１と、署名に用いた秘密鍵と対になっている公開鍵の証明書４０２をサービス提供部１０４に送信し、サービス提供部１０４に要求する（ステップ２０２）。ディジタル署名４０１を検証することによってユーザ認証を行なうことができるので、本実施の形態では認証子としてディジタル署名４０１を用いる。キャンセルする場合には「キャンセル」ボタン３０６を押す。

【００２１】基本認証部１０６では証明書４０２を検証し、正しい公開鍵を取得する。公開鍵を用いてディジタル署名４０１をチェックして利用者の認証を行なう（ステップ２０３）。正当な利用者であることが確認できた場合には、基本認証部１０６はデータ格納部１０７に対して要求されたデータの検索要求を渡し（ステップ２０４）、ポリシー管理部１０９に対してユーザＩＤを渡す。データ格納部では渡されたデータ要求に従って該当するデータを検索する（ステップ２０５）。本実施例では要求データ３０４として「ポンプとバルブ」を渡しており、ポンプとバルブの監視制御画面に関連するファイルを検索する。検索されたファイルの具体例を図５に示す。ファイル内のデータはタグによって特徴付けられている。

【００２２】ここで、<x>y</x>はデータyはタグxで特徴付けられている。この形式のデータファイルはＸＭＬ(eXtensible Markup Language)という標準的な記述言語がある。図５の場合、ｐｕｍｐタグ５０１ａはポンプの監視制御画面を構成する部品を内包し、監視画面を作るｗａｔｃｈタグ５０１ｂ、ポンプ起動制御を行なうｓｔａｒｔタグ５０１ｃ、ポンプ停止制御を行なうｓｔｏｐタグ５０１ｄを統括している。同様にして、ｖａｌｖｅタグ５０１ｅはバルブの監視制御画面を構成する部品を内包し、監視画面を作るｗａｔｃｈタグ５０１ｆ、バルブを開く制御を行なうｏｐｅｎタグ５０１ｇ、バルブを閉じる制御を行なうｃｌｏｓｅタグ５０１ｈを統括している。タグ５０１で囲まれたデータとして本実施例では監視制御を行なうための画面構成プログラム５０２を置いている。

【００２３】上記のタグ付きデータファイルはデータ変換部１１０に渡され、サービス利用部１０１に提示するデータを構成するための基本データとする。データ変換部１１０ではタグ５０１を読み取り（ステップ２０６）、該当するタグ５０１の付いたデータをサービス利用部１０１に提供してよいかどうかポリシー管理部１０９に問い合わせる（ステップ２０７）。ポリシー管理部１０９では、基本認証部１０６から渡されたユーザＩＤ３０１と、データ変換部１１０から渡されたタグ５０１からデータの提供に関する許可・拒否の判断を行なう（ステップ２０８）。

【００２４】この判断を行なうためのマトリックスを図６に示す。図６ではユーザＩＤ３０１ａ～ｃとタグ５０１ａ～ｈのマトリックスとなっており、マトリックス内の○×によって許可と拒否を表現している。例えば、ユーザＩＤ３０１がuser Aのユーザに対してポンプの監視画面を提供することは許可されているが、停止制御画面を提供することは拒否される。マトリックス中の条件文は情報提供を許可するための条件を記す。図６の条件文６０１ａでは、ユーザＩＤ３０１がuser Bのユーザに対してポンプ監視画面を提供するための条件として「ＩＦ　電源＝ＯＮ」と設定している。これは、ポンプの電源がオンの場合に限り、ポンプ監視画面を提供することを表す。同様にして、ユーザＩＤ３０１がuser Aのユーザに対してポンプ起動画面を提供するための条件として、時刻ｔが９：００から１７：００までであることを、条件文６０１ｂにて「ＩＦ　ｔ＞９：００　ａｎｄ　ｔ＞１７：００」として記述し、ユーザＩＤ３０１がuser Bのユーザにポンプ停止画面を提供するための条件として、ポンプの回転数が１００００未満であることを、条件文６０１ｃにて「ＩＦ　回転数＜１００００」として記述している。

【００２５】図３ではユーザＩＤ３０１がuser Bのユー

ザが「ポンプとバルブ」のサービス利用要求を出しており、これに対応して図５のタグ付きデータファイルが検索されたとする。データ変換部１１０では、ポリシー管理部１０９と連携して図７の形式の変換されたファイル７０１を形成する。ポンプの電源がオンで、ポンプの回転数が１００００未満の場合にはuser Bに対して、ポンプ監視画面、ポンプ停止画面、バルブ監視画面、バルブ閉画面の提示が許可されており、図７はＷｅｂで情報を提供する際のデータ形式であるＨＴＭＬファイルにしたものである。図７のデータを受信したサービス利用者がＷｅｂブラウザで閲覧したイメージを図８に示す。画面上には、ポンプ監視画面８０１、ポンプ停止画面８０２、バルブ監視画面８０３、バルブ閉画面８０４が表示される。一方、ポンプの電源がオフで、ポンプ回転数が１００００以下の場合には、ポンプ監視画面８０１、ポンプ停止画面８０２の提供が拒否されるので、サービス利用部１０１が閲覧できる画面は図９のようにバルブ監視画面８０３およびバルブ閉画面８０４になる。

【００２６】以上、監視制御画面を閲覧する場合について述べたが、一般の文書を閲覧する場合にも同様な処理が可能である。機密文書の閲覧要求に対して、データ格納部１０７からタグ付きデータファイルとして図１０のような機密文書１００１を検索したする。ここで機密文書１００１はｓｅｃｒｅｔタグ５０１ｉで管理され、セキュリティレベルに応じてｓ1、ｓ２、ｓ３タグをそれぞれ定義する。例えば、ｓ１タグ５０１ｊは社内秘レベル、ｓ２タグ５０１ｋは幹部レベル、ｓ３タグ５０１Ｌは役員レベルの機密情報として定義し、機密文書１００１を構成することができる。データ変換部１１０はこのタグ付きデータと、ポリシー管理部１０９への許可・拒否の問い合せにより提供可能なデータを再構成する。

【００２７】ポリシー管理部１０９では、図１１に示すマトリックスを用いて許可・拒否の判断を行なう。図１１は、ユーザＩＤ３０１がuser Aの利用者はｓ１タグ５０１ｉ付けされた社内秘データのみ閲覧可能、ユーザＩＤ３０１がuser Bの利用者はｓ３タグ５０１Ｌ付けされた役員データ以外は閲覧可能、ユーザＩＤ３０１がuser Cの利用者はすべてのデータが閲覧可能であることを示す。ここでデータ変換部１１０は、ユーザＩＤ３０１がuser Bである利用者に対してはｓ３タグで囲まれたデータを「＊＊＊＊」マークに変換して閲覧不能にしている。変換されたＨＴＭＬファイルの例を図１２に示す。データ変換部１１０から提供されたＨＴＭＬファイルは、先に述べたステップ２１０の暗号通信によりサービス利用者のアプリケーション実行部１０３に渡される。

【００２８】この画面表示例を、図１３に示す。ネットワーク上を流れるデータを第三者が盗聴した場合でも、暗号通信に用いる暗号鍵を復号化するための秘密鍵がなければ、図１０の画面の表示を防止することが可能になる。

【００２９】本実施の形態では、利用者が変わったり利用システムの状態が変わると、提供する情報も変化するところに特徴があり、機密保護、プライバシー保護を実現している。

【００３０】次に、サービス利用部１０１が利用システム１１１に対して安全に操作を行なう方法について図１４の処理フローを用いて説明する。例として図８においてポンプ停止ボタン８０５を押すことによって、ポンプ停止コマンドをサービス提供部１０４に送信する場合を考える。

【００３１】ポンプ停止ボタン８０５が押された場合、サービス提供部１０４とサービス利用部１０１で同期をとっている値とコマンドのセットを、一つのデータとしてアプリケーション実行部１０３は作成する（ステップ１４０１）。同期を取っているデータとしては時刻やカウンタなどが考えられる。

【００３２】図１５に示すようにコマンド１５０１は、タグ付きデータとする。コマンドであることはｃｏｍｍａｎｄタグ５０１ｍで示され、ｔａｒｇｅｔタグ５０１ｎがコマンドの送信先、ｐｕｍｐタグ５０１ａおよびｓｔｏｐタグ５０１ｃにより、ポンプを停止するコマンドであることを示す。「ａｄ％ｆ３８ｗｈ！ｆ７４」は、利用システム１１１に対して実際に送信されるべき制御信号１５０２で、利用システム１１１に依存する特別な値である。

【００３３】次に、タグ付きデータとしてのコマンド１５０１はユーザＩＤ３０１とカウンタ１５０３とともに、無作為に生成した暗号鍵を用いて暗号化され（ステップ１４０２）、暗号データ１５０４を形成する。暗号鍵はサービス提供部の公開鍵で暗号化する（ステップ１４０３）。暗号データ１５０４および暗号化された暗号鍵１５０５は、サービス利用部１０１の秘密鍵で署名される（ステップ１４０４）。アプリケーション実行部１０３では、暗号データ１５０４、暗号化された暗号鍵１５０５、署名データ１５０６、署名を検証するための電子証明書１５０７をセットにして基本認証部１０６に送信する（ステップ１４０５）。

【００３４】基本認証部１０６では、電子証明書１５０７を検証してユーザの公開鍵を取得し（ステップ１４０６）、署名データ１５０３を公開鍵で検証する（ステップ１４０７）。基本認証部１０６はサービス提供部１０４の秘密鍵を用いて暗号化された暗号鍵１５０５を復号化し、暗号鍵を得る（ステップ１４０８）。この暗号鍵を用いて暗号データ１５０４を復号化し、カウンタ１５０３とコマンド１５０１を得る（ステップ１４０９）。基本認証部１０６はカウンタ１５０３を利用履歴管理部１０５に問い合わせ、既に受信済みのものでないかどうかチェックする（ステップ１４１０）。受信済みであれば、コマンド１５０１を拒否し（ステップ１４１１）、受信済みでなければ、利用履歴管理部１０５に登録され

ている該ユーザのカウンタ１５０３を最新のものに更新し（ステップ１４１２）、コマンド１５０１をコマンド解析部に渡す（ステップ１４１３）。例えば、アプリケーション実行部１０３に保存されているユーザのカウンタ１５０３がｎであった場合、カウンタ１５０３の値をｎ＋１として添付する。送信されたカウンタ１５０３がｎ以下の場合には、送信データは既に受信済みであると判断して却下する。送信されたカウンタ１５０３がｎ＋１であればコマンド１５０１を認証し、利用履歴管理部１０５の登録値をｎ＋１に更新する。新規のカウンタ１５０３は、ユーザの公開鍵で暗号化されサービス利用部１０１に返信される（ステップ１４１４）。アプリケーション実行部１０３では、暗号化されたカウンタ１５０３を受信した場合に送達確認画面を表示し（ステップ１４１５）、ユーザの秘密鍵でカウンタ１５０３が復号化され、次のコマンド送信のために保存される（ステップ１４１６）。

【００３５】本実施の形態では、サービス利用部１０１とサービス提供部１０４で同期している値を用いて同じコマンドの複数回の受信を防止しているところに特徴がある。インターネットを使ったシステムの場合、ネットワークの途中で盗聴したデータをそのまま送信する再送攻撃という不正アクセス技術があり、これを防止する。

【００３６】また、誤って複数回ボタンを押してしまった場合にも、同じコマンドを複数受領することがなく、誤操作を防止することができる。また送信したコマンドが確実に利用システム１１１に送られたことも確認することができる。

【００３７】コマンド解析部１０８における処理フローを図１６に示す。コマンド解析部１０８は、コマンド１５０１のタグ５０１を解析し（ステップ１６０１）、ポリシー管理部１０９にタグ５０１の利用許可を問い合わせる（ステップ１６０２）。ポリシー管理部１０９ではユーザＩＤ３０１とタグ５０１、および利用システム１１１の状態に基づき許可・拒否の判断を行なう（ステップ１６０３）。拒否の場合には拒否である旨ユーザに通知し（ステップ１６０４）、許可の場合にはタグで囲まれた制御信号１５０２を利用システム１１１に送信する（ステップ１６０５）。

【００３８】本実施の形態では、制御信号１５０２をタグ５０１で囲んで送信することによって、制御対象（例えばポンプ）の機器毎にデータフォーマットが異なる場合（例えばＡ社はＸ方式、Ｂ社はＹ方式など）にも、制御対象自体が同じであれば同じ方式によってアクセス制御が行なえるところに特徴がある。

【００３９】

【発明の効果】以上述べたように、本発明によれば、利用者や利用システムの状態によって提供するコンテンツ自体を変化させ、機密保護、プライバシー保護を実現することができる。また、再送攻撃、誤操作を防止することができる。また、制御対象の機器毎にデータフォーマットが異なる場合にも、制御対象を同じタグで特徴付けることで同じ方式によってアクセス制御が適用可能であるところに特徴がある。

【図面の簡単な説明】

【図１】本発明を適用したサービス提供システムの全体構成図である。

【図２】本発明を適用したサービス利用者への情報提供処理の手続きを示すフローチャートである。

【図３】サービス利用部が利用者に対して提供する初期画面例である。

【図４】要求データ作成部において作成されるデータセットを示す図である。

【図５】データ格納部において格納されているプラント監視制御画面データの形式を示す図である。

【図６】ポリシー管理部において管理されているサービス提供を許可するか拒否するかを判断するルールを記述するマトリックスを示す図である。

【図７】データ変換部において変換されたプラント監視制御画面データの形式を示す図である。

【図８】データ変換部から渡されたプラント監視制御画面データを表示した画面例である。

【図９】ポリシー管理部において制限がかけられた場合の、データ変換部から渡されたデータを表示した画面例である。

【図１０】データ格納部において格納されている機密データの形式を示す図である。

【図１１】機密情報をどのユーザに許可するか拒否するかを判断するルールを記述するマトリックスを示す図である。

【図１２】データ変換部において変換された機密データの形式を示す図である。

【図１３】データ変換部から渡された機密データを表示した画面例である。

【図１４】サービス利用部からサービス提供部にコマンドを送信する処理の手続きを示すフローチャートである。

【図１５】サービス利用部からサービス提供部に送られるデータセットの模式図である。

【図１６】コマンド解析部における処理の手続きを示すフローチャートである。

【符号の説明】

３０１…ユーザＩＤ、３０２…パスワード、３０４…要求データ、３０５…ログインボタン、３０６…キャンセルボタン、５０１…タグ、５０２…画面構成プログラム、６０１…条件文、７０１…変換されたファイル、８０１…ポンプ監視画面、８０２…ポンプ停止画面、８０３…バルブ監視画面、８０４…バルブ閉画面、８０５…ポンプ停止ボタン、１５０１…コマンド、１５０２…制御信号、１５０３…カウンタ、１５０４…暗号データ

【図１】

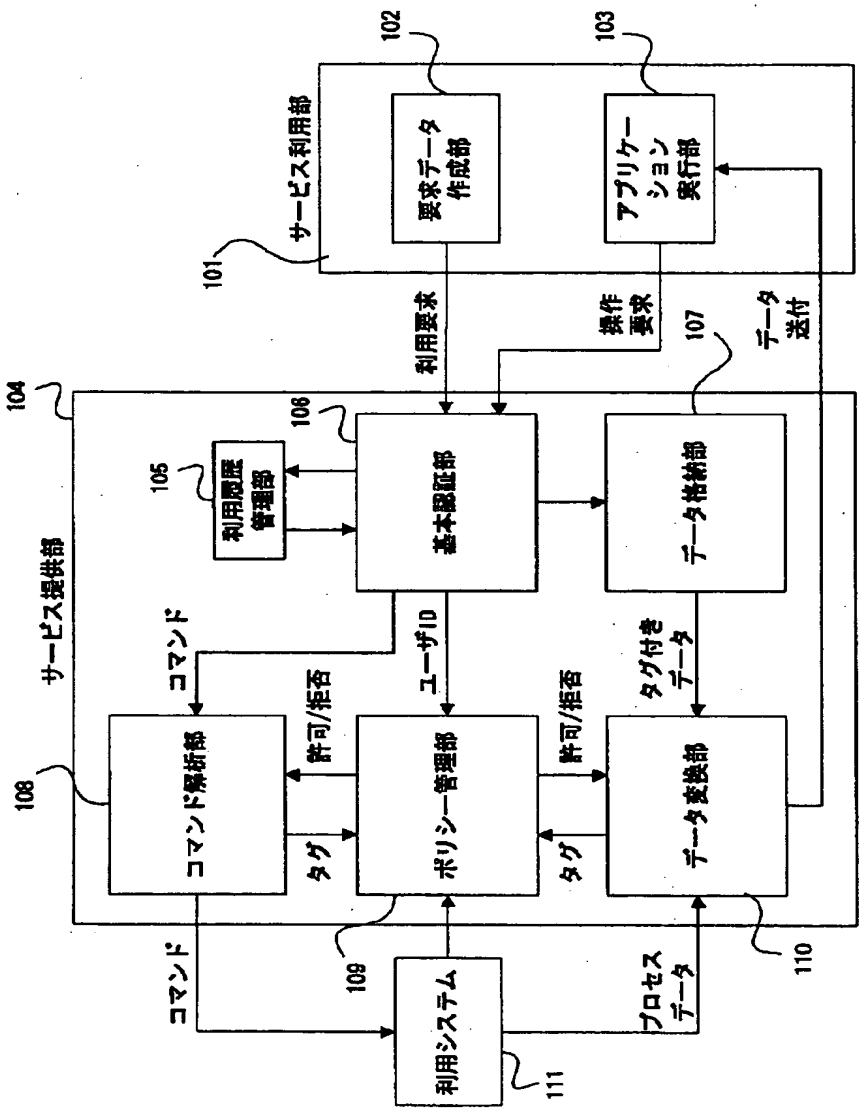
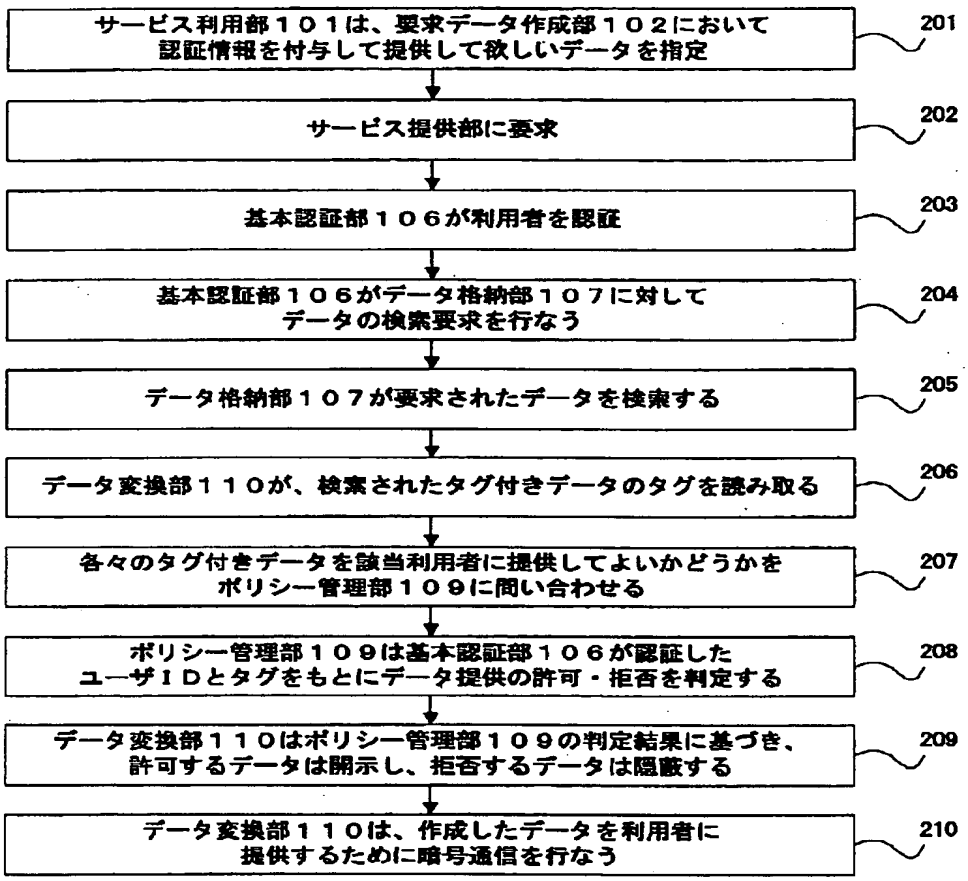

サービス利用部
101
要求データ作成部
102
アプリケーション実行部
103
利用要求
操作要求
データ送付
107
サービス提供部
104
利用履歴管理部
105
基本認証部
106
データ格納部
コマンド解析部
108
ポリシー管理部
データ変換部
コマンド
許可/拒否
タグ
ユーザID
タグ付きデータ
109
110
利用システム
111
プロセスデータ

図１

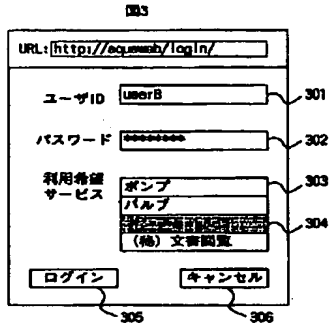
【図２】

図2



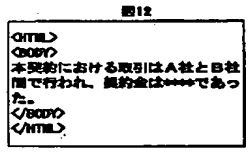
【図３】

図3



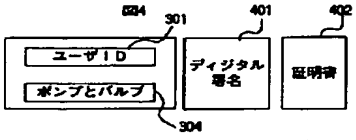
【図１２】

図12



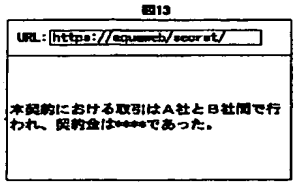
【図４】

図4



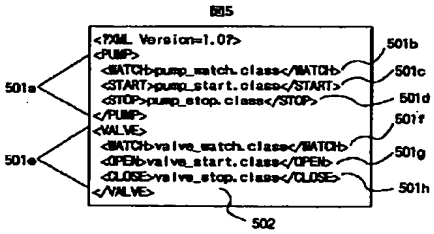
【図１３】

図13



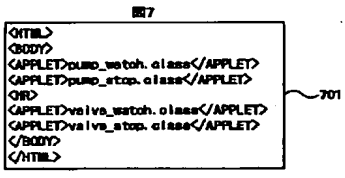
【図５】

図5



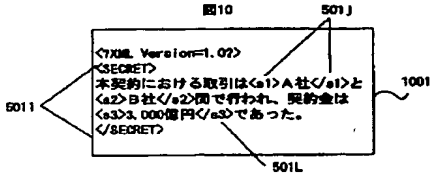
【図７】

図7

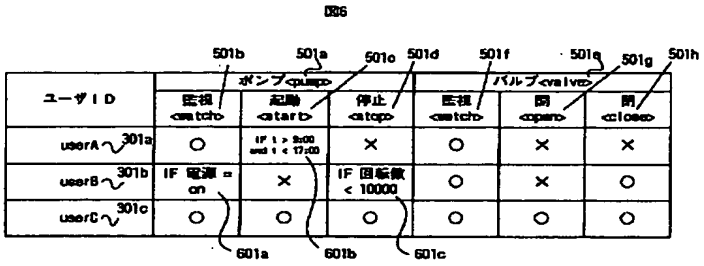


【図１０】

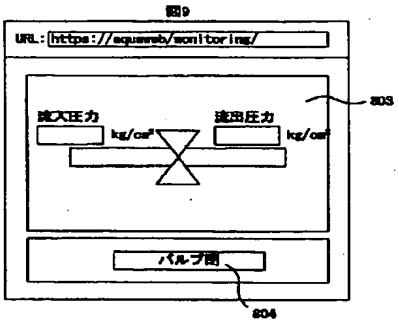
図10



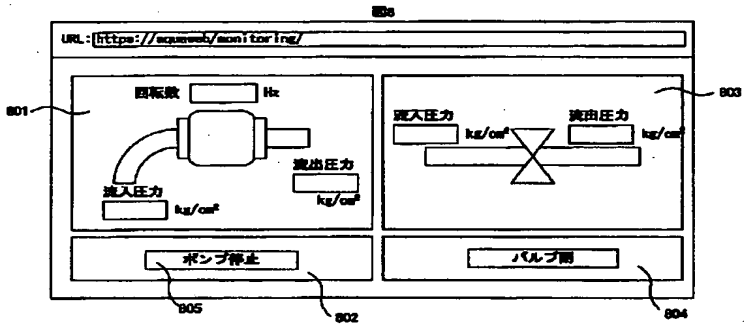
【図６】



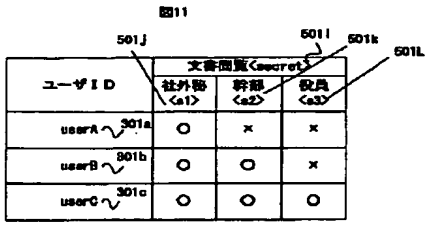
【図９】



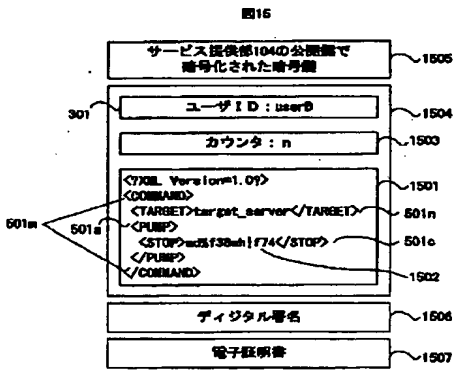
【図８】



【図１１】

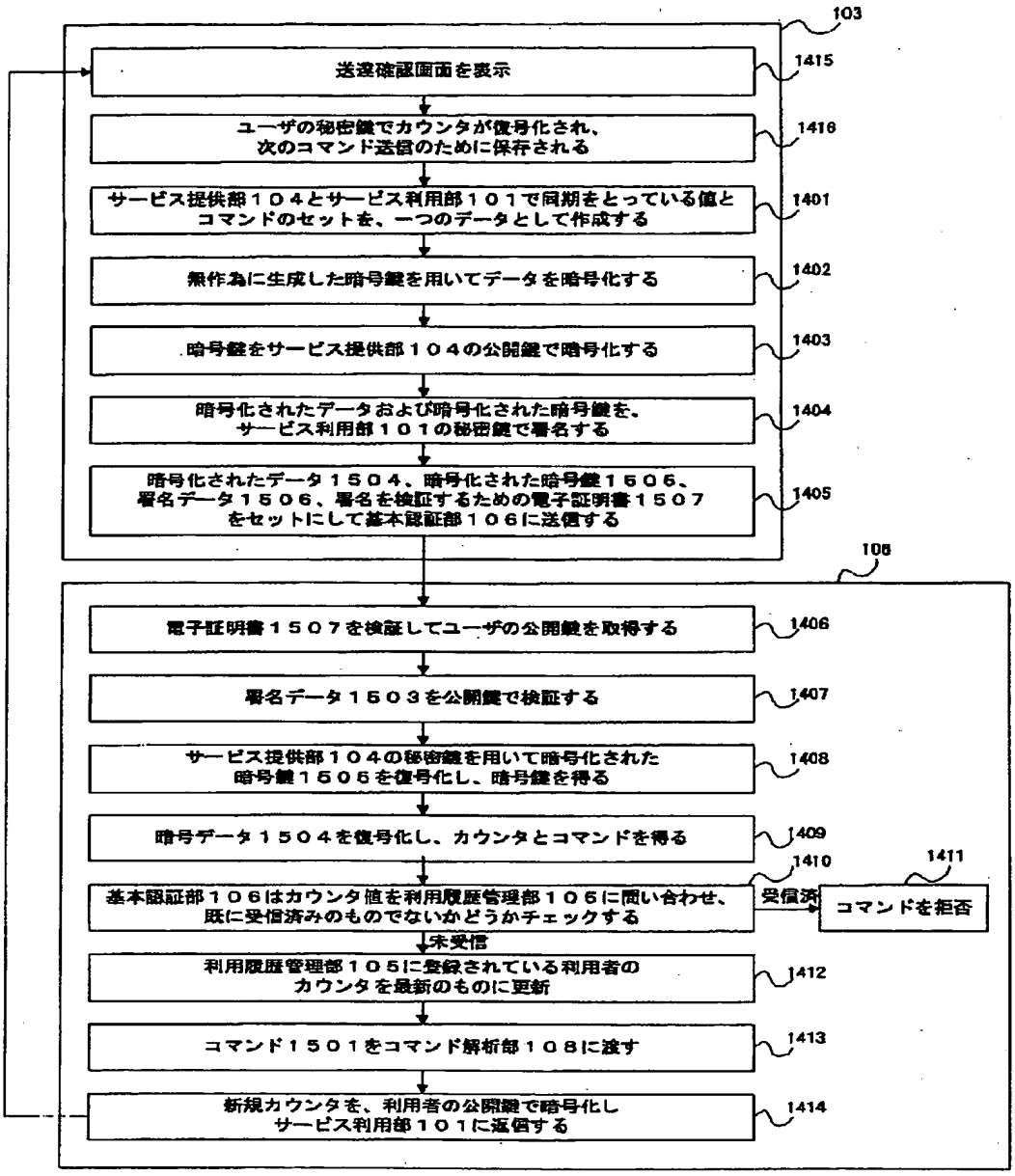


【図１５】



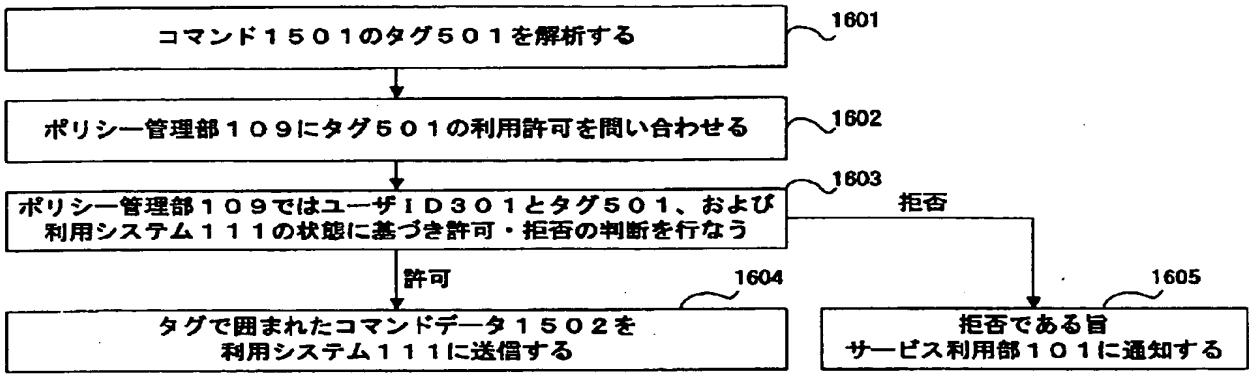
【図１４】

図14


103
送達確認画面を表示
1415
ユーザの秘密鍵でカウンタが復号化され、
次のコマンド送信のために保存される
1416
サービス提供部１０４とサービス利用部１０１で同期をとっている値と
コマンドのセットを、一つのデータとして作成する
1401
無作為に生成した暗号鍵を用いてデータを暗号化する
1402
暗号鍵をサービス提供部１０４の公開鍵で暗号化する
1403
暗号化されたデータおよび暗号化された暗号鍵を、
サービス利用部１０１の秘密鍵で署名する
1404
暗号化されたデータ１５０４、暗号化された暗号鍵１５０６、
署名データ１５０６、署名を検証するための電子証明書１５０７
をセットにして基本認証部１０６に送信する
1405
106
電子証明書１５０７を検証してユーザの公開鍵を取得する
1406
署名データ１５０３を公開鍵で検証する
1407
サービス提供部１０４の秘密鍵を用いて暗号化された
暗号鍵１５０６を復号化し、暗号鍵を得る
1408
暗号データ１５０４を復号化し、カウンタとコマンドを得る
1409
1410
基本認証部１０６はカウンタ値を利用履歴管理部１０５に問い合わせ、
既に受信済みのものでないかどうかチェックする
受信済
1411
コマンドを拒否
未受信
利用履歴管理部１０５に登録されている利用者の
カウンタを最新のものに更新
1412
コマンド１５０１をコマンド解析部１０８に渡す
1413
新規カウンタを、利用者の公開鍵で暗号化し
サービス利用部１０１に返信する
1414

【図１６】

図16



フロントページの続き

(51)Int.Cl.[7]		識別記号	F I		テーマコード(参考)
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｃ
	9/32				６７３Ａ

(72)発明者　瀬古沢　照治
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　宮尾　健
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所情報制御システム事業部内

Ｆターム(参考)　5B075 KK54 KK63 PQ02
5B085 AE06 AE23 BE07
5J104 AA07 AA09 AA16 EA05 EA06
EA19 KA01 LA03 LA06 MA02
NA02 NA05